Cybercore Integration Center

INL researchers working in the Cybercore Integration Center are improving the resiliency of the nation's critical infrastructure control systems.

Idaho National Laboratory's Cybercore Integration Center leads national efforts to secure critical infrastructure control systems from cyber threats. All critical infrastructures rely on industrial control systems to receive operational commands, process data, and perform essential services vital to our nation's security, lifeline services and the economy.

At Cybercore, multiple research and development initiatives seek to enhance the security and resiliency of industrial control systems by adopting an interdisciplinary approach to understanding the technical aspects of operational technology in an evolving threat environment. To achieve this goal, seasoned threat analysts work in concert with experienced power engineers, cyber researchers and control systems experts to develop novel, comprehensive solutions.

By utilizing INL's capabilities and partnerships to develop and deploy cyber-informed engineering methods and technologies, Cybercore integrates threat forecasts and consequence-based risk assessments that prioritize and protect the security and resilience of the nation's most essential operations. Our efforts create physical and virtual environments that accelerate the pipeline of engineers, operators and responders of cyber-physical systems.

STRATEGIC VISION

Secure global infrastructure from increasing cyber threats

- Partner across federal agencies, private industries, national laboratories and research institutions to rapidly advance control system cybersecurity.
- Accelerate workforce development to build a pipeline of control system cybersecurity talent.
- Drive a culture change in engineering to include security from the ground up.

SIGNATURE CAPABILITIES

- Expertise in leading control system technologies, vendors and implementations.
- All-source Technical Analysis of cybersecurity threats to controls systems.
- Malware and Forensics R&D of embedded systems analysis and reverse engineering.
- Hunt and Incident Response methodology for deploying intelligence-informed teams of cyber experts.
- Infrastructure Resilience and Interdependency Analysis for control systems, situational awareness and visualization R&D.

Idaho National Laboratory

FOR MORE INFORMATION

Director
Scott Cramer
208-526-2757
scott.cramer@inl.gov

Deputy Director of Operations
Sean McAraw
208-526-1394
sean.mcaraw@inl.gov

Deputy Director of Programs
Rob Helton
208-526-6266
robert.helton@inl.gov

Senior Advisor
Vergle Gipson
443-926-1721
vergle.gipson@inl.gov

www.inl.gov

A U.S. Department of Energy National Laboratory

- Assessments for asset owners, vendor devices and infrastructure systems.
- Training and Exercises to support workforce development programs.
- Nuclear-Cyber support for international training, policy development and domestic R&D.
- Power Grid effects modeling, testing and validation.
- Classified and Unclassified Lab Spaces to accommodate project-specific work at multiple classification levels.
- Wireless R&D and Testing for spectrum sharing, 4G/LTE industry-scale testing.

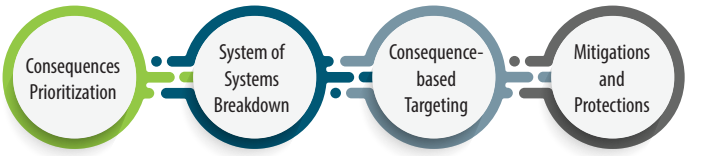
SPOTLIGHTED SERVICES

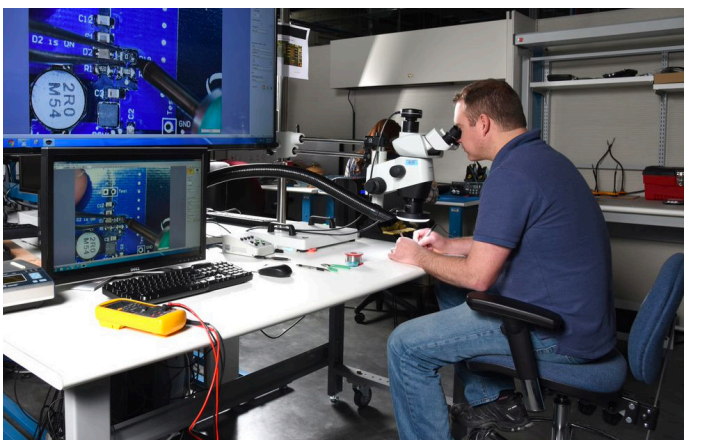
Cybercore offers its expertise in control systems, cybersecurity and power-related capabilities development to support multiple government agencies including the Department of Energy, the Department of Homeland Security, the Department of Defense and the Intelligence Community.

Notable initiatives include:

Consequence-driven Cyber-informed Engineering (CCE) employs an approach that assumes if a critical infrastructure network is targeted and adequate resources are leveraged, the targeted network can, and will, be penetrated. CCE's consequence-based risk analysis (attack path illumination) of the industrial control system environment helps critical infrastructure asset owners identify and create new engineering/design options, operational procedures, and active defense methods/alerts/safeguards.

CyberShock Workshops provide energy sector owners and operators hands-on experience with an industrial control system during a simulated cyber attack. Drawing on elements from multiple cyber attacks on control systems, the CyberShock platform challenges participants to defend against a cyber attack on control equipment they routinely use.





LEVERAGED INL RESOURCES

INL's 890 square mile desert Site offers utility-scale research, development, testing and training opportunities utilizing unique assets:

- Isolatable 16-mile, 138 kV and below Electric Power Grid Test Bed with multiple substations.
- Commercial-grade Wireless Test Bed with NTIA experimental radio station status.
- Commercial and residential-grade Water and Pipeline Security Test Bed.
- Cyber and control systems research and development laboratories.
- Operational transportation network including fleet vehicles, dispatching, roads and bridges.
- Large-scale, operational manufacturing facility.

EXPANSION

Soon, INL will open a state-of-the-art facility to house the Cybercore Integration Center. This 80,000 square foot facility will be equipped with secure office space and laboratories and leverage relationships with leading industry cybersecurity companies, universities and thought leaders to create the nation's preeminent resource for control system cybersecurity.

20-50444_003_R0